U.S. NAVAL WAR COLLEGE
Newport, Rhode Island

Naval Intelligence Policy for Support to Information Operations

by

Michael S. Grogan

Major, United States Marine Corps

A paper submitted to the Faculty of the Naval War College in partial completion of requirements for the Department of Joint Maritime Operations.

6 August 1998

Professor Fred Farmer
CCE JMO Instructor

Naval Intelligence Policy for Support to Information Operations

Why Information Operations?

Information Operations (IO)[1] seek to provide friendly forces with information superiority over their adversaries, despite adversary efforts to deny that advantage in favor of their own forces and activities. New operational concepts -- such as combined maneuver, precision strike, and battlespace awareness -- offer improved military effectiveness with minimum collateral damage and casualties.

IO have gained increased interest within the Department of Defense (DoD) and US Naval forces for their potential use at all levels and across the warfare spectrum—peacetime, MOOTW[2], and open conflict. It is imperative that Naval professionals thoroughly understand the IO medium and who they can counter our adversaries use against US forces, while successfully utilizing IO in support of US operations. Likewise, intelligence support to naval operations demands that intelligence professionals understand the intelligence requirements and support that IO demand. But these operations also demand a greater flow of information and information of greater granularity than ever before in order to ensure dominance of a given battlespace. The force that is able to collect, process, and transmit this information accurately to its units gains a very significant advantage over a force which cannot. Actions we may take to preserve the integrity of our own information, information-based processes, and information systems, while degrading the adversary's information and systems will create an information differential over opposition forces. In essence, this *is* information operations.

It is important to note that these disciplines are not new, and their integration is not new. IO occurs in a historical context. Sun Tzu wrote:

> *All warfare is based on deception. Hence, when able to attack, we must seem unable; when using our forces, we must seem inactive; when we are near, we must make the enemy believe we are away; when far away, we must make him believe we are near. Hold out baits to entice the enemy. Feign disorder, and crush him*[3].

---

[1] Information Operations consist of actions taken to affect adversary information and information systems while defending one's own. (JP 3-13 Draft)
[2] Military Operations Other Than War. (JP 1-02)
[3] Sun Tzu, *The Art of War*, trans. S. B. Griffith (New York: Oxford University Press, 1982).

Thus, IO is not new. But the present revolution in information technology so affects the means by which information superiority may be gained that the familiar methods by which we have pursued this advantage are rendered obsolete. For this reason, we must reevaluate our methods and our position in the competition for information superiority, just as if the competition were new. There are several key areas that characterize the *new* competition.

First, the speed with which advanced commercial information technology is proliferated and integrated within the military force is key. Since all military forces are increasingly dependent on commercial development of applications, they draw from a common information technology base. Given the phenomenal rate of technical advance in this area, a force that does not quickly acquire and adopt upgraded information technology will soon find its technology obsolete. Success in this area is determined not only by acquisition policy, but also by doctrine, training policy and the resource priorities assigned to information technology.

Second, the range of potential mission areas is important. Forces challenged by operating in a very wide range of missions worldwide, including non-traditional missions -- such as peacekeeping and humanitarian operations -- are disadvantaged when compared to forces with a narrow range of potential opponents. A narrow focus makes it much easier to develop militarily significant information on the adversary, while preserving the availability and integrity of one's own information resources. The range of missions assigned is a political consideration, but strong operational security doctrine, training, and the availability of high-quality intelligence will directly affect success across the spectrum of missions.

Finally, the degree to which key military information structures are protected is also important. Defense structures are intertwined with, and dependent upon, the national and transnational global information infrastructure (GII)[4]. This complicates their defense, because networks are like the proverbial chain with a weak link; they are no more secure than their least-secure node. Success in this area would be enhanced by dedicated military networks or, failing this, adherence to fairly robust commercial network security standards. But this second action requires cooperation and investment by commercial-service providers, whose investment decisions are guided by competition. Beyond that required for loss prevention,

[4] Global information infrastructure consists of the worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the GII. (JP 1-02)

it is not clear that there is any commercial competitive advantage to be gained by security investments. For this reason, market forces are unlikely to answer DoD's security needs unaided.

Naval Intelligence must be postured to support all dimensions and applications of IO. Naval Intelligence officers, specialists, and civilian personnel--serving afloat and on shore, in Navy and Joint commands--must provide tailored intelligence to diverse customers involved in IO. These customers include the research and development, acquisition, policy, doctrine, strategy, and operations communities; the intelligence community; and the warfighter at the tactical, operational, and strategic levels. This will require a dedicated effort by all involved working toward common goals from a common understanding of the unique contributions IO make to military forces.

Information Operations and the Role of Naval Forces

IO involve actions taken to affect adversary information and information systems while defending one are own. The ultimate objective is to influence decision-makers. An IO is used as an enabler and force multiplier, utilizing single disciplines across the spectrum of civil-military operations from peace to crisis to conflict, and at all levels of war. At the strategic level, IO will be directed by the NCA[5] to achieve national objectives by influencing or affecting key facets of an adversary's power. Naval forces, as a forward-deployed element of our national power, will conduct IO at the operational and tactical level to achieve or support national objectives. These operations consist of offensive IO, defensive IO, and related peacetime and pre-crisis activities such as civil affairs and public affairs.

US Naval forces provide sovereign, forward deployed options needed for various IO systems and activities. Peacetime IO can influence adversaries, shape the strategic environment, and reinforce adversary perceptions of our missions and intentions. Pre-crisis preemptive or retaliatory IO can deter adversaries from initiating actions detrimental to our interests. During combat operations involving forward deployed naval forces, IO will help prepare the tactical and strategic battlespace by:

- Acting as levers to increase combat power by achieving information superiority
- Supporting maneuver warfare

[5] National Command Authority (JP 1-02)

- Creating non-linear dynamics with disproportionate (asymmetric) outcomes in our favor
- Attacking every aspect of an adversary's information flow via--among other means--physical destruction; logic attacks on critical nodes; jamming; surgical denial of military communications, sensors, and navigation aids; and intrusion into or usurpation of networks and databases
- Supporting deception by introducing through signature manipulation and other means (including maneuver) false images of reality into the adversary's perceptual apparatus
- Employing reflexive control over the adversary by reinforcing his predisposition and assumptions, thereby contributing to surprise or even making it inevitable

The ultimate effect of these IO is to manipulate or usurp the adversary's cognitive processes and understanding of reality. Naval forces employing IO in effect engage in a form of cognitive maneuver in the spatio-temporal dimension, the principal focus of which is the enemy commander, his decision making process, and those targets related to C4ISR[6] and other critical information-based processes which are fundamental to conducting modern military operations. When thus employed as an integrating strategy, IO focuses on the considerable vulnerabilities and opportunities represented by military forces' increasing dependence on information and information systems.

About the Information Operations Threat

Almost all of the current IO threat discussion is about computer warfare, specifically the vulnerability of our computers and networks to attack, rather than about IO in its fullest sense. Recalling that IO is the integration of psychological operations (PSYOPS)[7], deception, destruction, electronic warfare (EW), and operations security (OPSEC)[8], the focus on computers is incomplete, if understandable. An IO threat would question whether our information environment could be manipulated by others to gain information superiority over us by whatever means, including computers but not limited to them. Currently, there are a meager few who are doing the work of screening for occurrences of foreign manipulation of our media. However, the numbers of events using this IO tact, which have been detected, are both impressive and indicative that we should be looking more comprehensively for such manipulation. Likewise, foreign use of counter-deception and counter-psychological operations against US interests raise similar concerns.

---

[6] Command, control, communications, computers, intelligence, surveillance, and reconnaissance. (JP 1-02)

[7] Psychological operations are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, which ultimately induce or reinforce attitudes and behavior favorable to the originator's objective. (JP 1-02)

[8] Operations Security is a process of identifying those actions by your own friendly forces which can be observed by adversary intelligence systems and to determine indicators hostile intelligence systems might obtained to discern your operational plans.

Even limited to computer network attack (CNA)[9], popular perception of the IO threat is probably exaggerated. The vital infrastructures, especially the communications infrastructures of the US are robust, diverse, and designed to respond flexibly in natural disasters and other calamities. Further, one needs spend only a little time reading hacker computerized bulletin boards and internet news groups to conclude that the majority of hackers are *sociopathic braggarts*--the computer equivalent of graffiti artists--who seek to gain notoriety. If our networks were as vulnerable as some assert, the "electronic Pearl Harbor" that many fear would have occurred by now, and would have been widely publicized, with hacker *noms-de-cyber* claiming credit for the event. Some will argue that we cannot know for certain that there is not someone out there in the GII who could mount such an attack. While that is technically true, it does not prove the affirmative, that there really is such a person or group.

In addition, there are other reasons to believe that the threat is not all that some advertise it to be. We know from IO "Red Teaming" -- in which we attack our own systems to find their vulnerabilities -- that it is very difficult to target a CNA on any particular system. An ideal weapon fires when you pull its trigger, transverses the battlespace to the target you intend, and causes the damage to (hopefully) the extent you desire. The key attributes are controllable time, location, and effect. Few IO red team tools could meet these criteria now. It is very doubtful that potential adversaries have been able to do any better, because to do so, they would have to conceive and develop more effective attacks on our systems than we have been able to do ourselves, using detailed engineering-level understanding of those systems. An irony of IO is that it is almost always possible to do something, somewhere, sometime; but it is only rarely possible to do a specific thing, at a specific location, at a specific time. That makes the use of IO tools particularly challenging for military planners.

This is not to say, however, that there is no threat, or that those who are concerned about defending our nation against an IO attack are wrong. The probability of a nuclear attack on the US is very low, however the cost of such an attack in terms of lives and damage to our national well being is unacceptably high. Thus, we have a well-developed indications and warning system, robust command and control, broadly understood deterrence policy, and other measures to mitigate an unlikely, but unacceptably costly,

---

It also encompasses your actions to eliminate and reduce these indicators to counter adversary exploitation. (JP 1-02)

[9] Computer network attack. Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (JP 3-13 Draft)

nuclear attack. Similarly, the likelihood of a widespread IO attack on the US is probably very low, but the impact of such an attack on our national well being is unacceptably high. We must have similar mechanisms to mitigate this small, but unacceptably costly, IO risk.

One interesting corollary of IO is that it may be more appropriate to low-level conflict than it is to general war, given its current state of development. There are several reasons why this is true. The opportunity cost to obtain a CNA capability is relatively low, certainly far less than the cost of obtaining a conventional attack capability, which could threaten the US. Further, an IO attack may be non-lethal and non-attributable to the perpetrator. It may manifest itself in the same way if originated by an adversary ranging from a nation-state to an individual, and would almost certainly impact information structures that are not traditionally considered to be a DoD responsibility, thereby falling into an interagency gap in responsibility. Thus, an IO capability is an attractive choice for a wide range of potential adversaries, including traditional military opponents, but also non-state actors and even economic competitors. In this context, almost any state or organization can be an IO threat, so all must be considered potential IO competitors.

Because of their low opportunity cost and the relative ease with which CNA tools may be used in harassing or terrorist-like operations, these capabilities are very likely to be of interest to hostile non-government organizations (NGOs). For IO, hostile NGO's are also advantaged by several other factors. Specifically, they generally lack territory that can be threatened with conventional military retaliation. Thus, our best-understood and most robust countermeasure is rendered ineffective. Also, their non-governmental status and the type of threat that they pose raises unresolved questions about which US government agency is responsible to defend against their actions. Some hostile NGO-sponsored attacks might be considered to be a law enforcement responsibility and, depending on the target attacked, might fall under either federal, state or some combination of jurisdiction. In many cases, intent would be the major determinant and, of course, intent may be impossible to determine. This administrative question is non-trivial; because an attack on our information networks could occur very rapidly, leaving little time for agencies to debate about which should take what action. Thus, this lack of definition is certain to hamper response by whatever agency is finally assigned responsibility, and virtually assures the hostile NGO freedom of action in the early stages of the attack. Thus, like a terrorist cell, the hostile NGO may be quite small, with members well known to each other, complicating any law enforcement action. But, unlike the

typical terrorist scenario, a hostile NGO planning a CNA doesn't need restricted technology or material -- no explosives, for example, are necessary. Rather, the CNA tools are likely to be the same as those used in many businesses -- computers and computer-based information. Thus, before and even after the attack, there is very little physical evidence to link the hostile NGO with the action.

Offensive Information Operations

Offensive IO target the human and technical means which adversary makes decisions. They represent a fusion of target sets that include foreign decision making styles (human/cognitive factors) as well as automated systems used to provide information to the decision-makers. Offensive IO involve the integration of varied capabilities and activities including EW, OPSEC, military deception, PSYOPS, physical destruction, and CNA. Certain offensive IO activities may be conducted in peacetime or pre-crisis situations with the goal of communicating information and providing support to critical audiences to influence their understanding and *perception*, and to help shape the strategic environment. These IO may include activities taking place over an extended period of time intended to give U.S. forces leverage over potential adversaries in crisis, conflict, and conflict resolution situations. To achieve their full potential, such IO require planning and implementation over a long period of time from peacetime (primarily perception management efforts) and crisis (deterrence measures) through wartime (active and passive IO and command and control warfare). The primary targets of these IO are not so much an adversary's technical information systems as his decision making process and strategic mindset. Hence consistency of message and effort is critical because perception management and crisis deterrence measures have at their core a significant degree of truth that should be allowed to degrade gracefully rather than fail catastrophically.

Defensive Information Operations

Defensive IO involve all activities designed to protect information and defend information systems, as well as allowing US decisionmakers to *accurately anchor their perception* of the truth correctly. Defensive IO are conducted through physical security, OPSEC, counter-deception, counter-psychological operations, counterintelligence, electronic protect, and information assurance (IA). IA protects and defends information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation through use of tools and capabilities for verification of information, assurance readiness, and robustness in an operational environment. IA includes providing for restoration of

information systems by incorporating protection, detection, and reaction capabilities.

Naval Intelligence Imperatives

IO involving forward-deployed naval forces require continuous intelligence support from ship and shore. Traditional intelligence preparation of the battlespace (IPB)[10] is the foundation of this support, and must provide detailed knowledge of the adversary's use of information and information systems. Fundamental to this effort is the requirement to work with the operator and strategist in developing targets sets and priorities within the context of the operational realities facing fleet forces. Therefore, IPB (in the context of offensive IO) requires knowledge of information systems and the human decisional interface with those systems. This includes an understanding of the adversary's cultural, political, and social beliefs and values such that his response to an IO "message" can be predicted and its risk weighed in the larger context of tactical and strategic security (escalatory) implications. It further includes an understanding of the adversary's decisionmaking process; and an understanding of the biographical background of key adversary leaders and decisiomakers, to include motivating factors, leadership style, and vulnerabilities. One of the greatest challenges for intelligence support is to develop measures of effectiveness for IO in order to conduct battle damage assessments that will not compromise the source or sensitivity of the IO activities. Defensive IO require intelligence not only to identify the physical threats to naval forces' information and information systems, but also to try to understand and predict adversaries' intentions and likely responses to physical denial of their IO actions against us.

Indications and Warning Requirements and Methodologies

Naval Intelligence, as a part of the national ***Indications and Warning(*** I&W) community, must be prepared to identify the intelligence signatures of IO activity and their potential impact on naval forces and facilities. The pillars of IO--physical attack, EW, PSYOPS, deception, and OPSEC--have the same intelligence signatures both as traditional warfare disciplines and as elements of IO. Strategic IO, however, especially as CNA based anywhere in the world (or beyond it), can bypass forward deployed defense forces and I&W systems and strike directly at critical targets without revealing their genesis through known intelligence indicators. The significance of such events demands *continuous* Naval Intelligence participation in the national intelligence community's development of a means for analysts to characterize all-source data and provide strategic warning to decision makers against the potential for a stand-alone CNA. The basis of

[10] Intelligence preparation of the battlespace is an analytical methodology employed to reduce uncertainties concerning the

an IO warning matrix relevant to naval forces includes the general factors of capability, history, intentions, and targeting, all of which must be thoroughly understood by Naval Intelligence professionals involved in I&W at all levels:

- Capability: Of special relevance to naval forces is the potential for threats that result in both widespread, long-duration damage and short-duration, high-impact damage to critical elements of a deployed force's information infrastructure.

- History: Past operational practices of the state/nonstate actor, to include use of CNA and other elements of IO such as deception and electronic warfare in a maritime environment.

- Intentions: Elusive and difficult to gauge yet fundamental to anticipating the phenomenology of IO events, knowledge of a potential threats intentions is achieved only through rigorous and dedicated analysis of both overt statements and information obtained via classified sources or observed during exercises and training.

- Targeting: Requires the expertise and sophistication to recognize evidence of preparations to execute IO, especially CNA.

IO indicators that are particularly relevant to naval forces and operations, and which the emerging national intelligence community I&W methodology is designed to track, analyze, and report on, include several key items. Intelligence operations conducted within and outside the United States that are directed against any aspect of the US national information infrastructure. Examples include: expressions of a desire for--or the establishment of--foreign offensive IO operational and/or contingency plans; the detection of computer probes and intrusions of critical US information systems and networks; and attempts to introduce hostile computer modifications into any critical US information system or network. Further examples include foreign attempts to recruit US personnel to assist in the possible penetration of critical information systems or networks; cooperation or collusion in the development of offensive IO capabilities among nations and/or non-state groups known to be hostile to the US interests; disruption or denial of international telecommunications access to any foreign countries; and foreign targeting of US space-related ground facilities, equipment, or personnel.

Collection Support

Closely related to the requirements for I&W are those for collection support. Naval Intelligence professionals involved in collection activities must be thoroughly familiar with the overall collection goals.

---

enemy, environment, and terrain for all types of operations and is a continuing process. (JP 1-02)

Specific IO collection objectives and responsible national intelligence agencies are enumerated in national collection directives, but at a minimum, Naval Intelligence--even as a secondary action office in most IO-related collection areas--must intensify its collection efforts against the following generic requirements and tasking, given their importance in the maritime environment.

Examples of collection interests might include: foreign state and non-state actors' policies, plans, programs, and doctrine to conduct offensive IO; the purchase of dual-use technologies which could be used in the development of IO weapons; foreign leadership (especially military) use of information infrastructure and information-based decision making processes in the preparation for and conduct of IO, with emphasis on armed forces' command and control as it relates to IO; and foreign offensive IO capabilities to attack U.S. military information systems and infrastructures, especially technical attack capabilities against computer systems and command and control targets, and against other military systems that are heavily dependent on computer technologies

In addition to focusing analytical and collection personnel and resources required to satisfy these requirements, Naval Intelligence should develop a dedicated all-source collection/exploitation capability for tracking foreign requests-for-proposals, specifications, contract awards, as-built configurations, software (both off-the-shelf and standard), and data protocols for militarily significant information systems. This would involve a methodology similar to that employed in the maritime civil fleets arena for tracking sensitive cargoes, but would not be limited to items carried in ships or purchased by foreign navies, and would encompass instead strategic information systems which the U.S. Navy might be responsible for attacking/influencing.

Analytic Support

Intelligence research and analysis are the acknowledged foundation of all planning, strategies, concepts of operation, and acquisition activities in support of IO. In order to ensure the success of Navy and Joint IO, Naval Intelligence professionals in analytic and management billets--and the organizations housing them--must direct their research and analysis to satisfying the unique operational and strategic requirements discussed above. Analysts at all intelligence collection levels must integrate IO requirements into their routine activity by expanding the traditional scope of their research and becoming responsive to all-source derived data that pertain to IO.

The overarching goal of this effort is the development and maintenance of an evidentiary and knowledge base, which will be the starting point of Naval Intelligence analytic support to IO. The primary production vehicles will be studies containing tailored information upon which military actions across the spectrum from peacetime engagement to warfare termination can be undertaken with a high degree of confidence in their success. These studies will be of all potential IO actors--nations, subnational groups, ethnic or tribal entities, and transnational groups--against which forward deployed naval forces might engage in IO. The studies must be relevant to naval and joint military operations in peacetime deterrence, crisis management, and escalation control/dominance in armed conflict. These studies must act as "target folders" containing detailed descriptions of both military and civil information infrastructures to the requisite level of granularity and timeliness so as to be employed by decision makers and operators during a crisis, at the brink of conflict, throughout a conflict, and for conflict termination leverage. Likewise, they may be used identify exploitable vulnerabilities, adversary perceptions that can be manipulated, and the probable outcomes of IO employed by naval forces in a given scenario. Furthermore, these IO studies could become invaluable in supporting long-term peacetime strategic IO designed to influence and control a potential adversary's perceptions of US military capabilities and intentions in a crisis or conflict.

To accomplish this will demand a level of knowledge and understanding of potential adversaries. Knowledge of their information infrastructures that can only be derived from dedicated analysis of targetable information technologies, military exercises, sensitive doctrinal writings, public statements and writings, leadership decisionmaking culture, and biographical analyses that focus on an individual's potentially exploitable roles in his command and control environment. These studies will incorporate the results of all relevant analyses in support of IO undertaken by Naval Intelligence and other intelligence community professionals. These studies could serve as information repositories of the accumulated intelligence community knowledge relevant to IO in a maritime and expeditionary warfare environment. They would become "go-to" manuals viewed by Navy and national decisionmakers as prerequisites for concepts of operations, measures of effectiveness and feasibility assessments, and the real-world decisions to commit naval forces to action in crisis or conflict. Such studies therefore will help prepare the battlespace not only in a tactical sense but also as the foundation for U.S. Navy strategy, and will capitalize on Naval Intelligence's experience in supporting IO endeavors at the strategic level.

Strategic IO, so named by virtue of their national security implications, may be broadly defined as perception management and foreign leadership influence programs and operations. The focus of naval activity in strategic IO can begin years in advance of an anticipated engagement. Successful strategic IO will be the product of a deliberate and lengthy coordination process involving many levels of approval and occasionally non-DoD agencies. The ultimate goal of this intelligence support will be to accomplish the following:

- Identify potential US adversaries who can be successfully be targeted by strategic IO.
- Determine the preferred US strategies to influence or deter adversaries IO pursuit.
- Assess the relevance of naval capabilities to promote or deter an adversaries IO activities.
- Identify adversaries perceptions about the Navy which we can use to promote desired, and deter undesired, adversary intentions and activities.
- Identify adversary perceptions and intelligence that would contribute to the effectiveness of crisis response deterrent actions and the performance of US Naval forces in combat.

Conclusion

In conclusion, it is clear that Information Operations raise many policy and planning issues, but it also offers remarkable potential. United States naval forces are challenged with an extremely broad range of missions today, many requiring non-lethal or less-lethal capabilities. Faced with increasingly diverse military operations within a declining resource environment, we must find ways to make our remaining force structure more effective. IO can be a force multiplier and an inexpensive one, as well. Finally, we are engaging these notions at a time when the Cold War paradigm of deterrence through "Mutual Assured Destruction" is replaced by a national security strategy of engagement and peacekeeping. IO offers the possibility that we might be able to preserve or restore peace through non-lethal -- in current defense parlance, "non-kinetic" -- means. It is this last possibility that is most enticing, because it could lead to a practical enhancement of the military role in and capability to maintain the peace, one that would do so without unduly risking the lives of our servicemen and women. Equipped with an appropriate array of IO tools and the policy structure to use them, we might imagine a theater Commander-in-Chief training to wage peace, as we once trained for war. All of this is possible, and an appropriate response to our changing missions in a changing environment.